

文系の、文系による、文系の為の 現代暗号基礎



-BaalzeBuB-



あぢえんだあ？

- 暗号の基礎用語
- 暗号方式の分類
- 暗号方式の歴史
- 新時代の幕開け
 - 秘密鍵暗号方式
 - 公開鍵暗号方式
 - ハイブリッド



暗号の基礎用語

- アルゴリズム
 - データを暗号化する為の手順・処理方法
例：金庫を開けるのにツマミを回す
- 鍵
 - 処理の深度
例：ツマミを何回どっちに回すか



暗号方式の分類

- 転置式

 - 例：シーザー式暗号

- 換字式

 - 単語単位での置き換え (Code)

 - 文字単位での置き換え (Cipher)

 - 混合方式 (Nomenclature)

- 隠字式 (Steganography)

 - 例：炙り出し、埋め込み画像



暗号方式の歴史

- 手作業での暗号、復号化
 - 文書の隠匿
 - シーザー式転置暗号
 - Codeの登場
- 産業革命、機械の時代へ
 - WWII(紫暗号、エニグマ暗号)
- そして、電子の時代へ



新時代の幕開け

- 秘密鍵暗号方式
 - 鍵は秘密です（笑）
- 公開鍵暗号方式
 - 対となる2つの鍵を使用する
 - 一方の鍵で暗号化されたデータは他方の鍵でのみ復号化が可能
 - 一方の鍵から他方の鍵を推測する事が困難
- ハイブリッド方式
 - 公開鍵方式で秘密鍵を交換する



現代暗号の特徴

- 秘密鍵暗号方式
 - 長所：暗号化処理の負荷が小さい
 - 短所：鍵交換が難しい
- 公開鍵暗号方式
 - 長所：鍵交換の必要が無い
 - 短所：暗号化処理の負荷が大きい
- ハイブリッド方式
 - 萌えてます、(´ー`)ノ

いじよ。



蠅